AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

Claims 1-10. (Cancelled)

11. (Currently Amended) A method for generating a public key certificate of an end entity by a registration authority and an issuing authority in a public key infrastructure, comprising the steps of:

generating, by the registration authority, a signature to contents to be registered with a public key certificate, ~~certificate and,~~ and a certificate issuing request including both the contents signed by the registration authority and a signature to the contents signed by the registration authority;

sending the certificate issuing request from the registration authority to the issuing authority;

generating, in response to the certificate issuing request by the issuing authority, a public key certificate including the contents signed by the registration authority, the signature to the contents signed by the registration authority, issuing contents to be issued by the issuing authority, and an issuing authority signature to the contents signed by the registration authority, the signature to the contents signed by the registration authority and the issuing contents issued by the issuing authority; and

sending the public key certificate from the issuing authority to the registration authority for being registered within the registration authority.

12. (Previously Presented) A method as recited in claim 11, wherein

the contents signed by the registration authority is a predetermined identifier to specify information to be certified by the pubic key certificate of the end entity.

13. (Previously Presented) A method as recited in claim 11, wherein

the contents signed by the registration authority is a hash value calculated by applying a hash function to information to be certified by the public key certificate of the end entity.

14. (Previously Presented) A method for as recited in claim 11, further comprising the steps of:

verifying, by a verifying party, the issuing authority signature with the contents signed by the issuing authority; and

verifying, by the verifying party, the registration authority signature with the contents signed by the registration authority included in the public key certificate.

15. (Previously Presented) A method as recited in claim 12, further comprising the steps of:

acquiring, by a verifying party, information signed by the registration authority according to the identifier in the public key certificate;

calculating, by the verifying party, a hash value of the acquired information;

decoding, by the verifying party, the registration authority signature included in the public key certificate, by using a public key of the registration authority; and

checking by the verifying party, whether the hash value is identical to the decoded value.

16. (Previously Presented) A method as recited in claim 13, further comprising the steps of:

calculating, by a verifying party, a hash value of the information signed by the registration authority in the public key certificate;

decoding, by the verifying party, the registration authority signature included in the public key certificate, by using a public key of the registration authority; and

checking by the verifying party, whether the hash value is identical to the decoded value.

17. (Previously Presented) A method as recited in claim 14, further comprising the steps of:

constructing and verifying, by the verifying party, a path from the certificate authority trusted by the verifying party, up to the public key certificate;

verifying, by the verifying party, the registration authority signature described in the public key certificate using the public key of the registration authority; and

constructing and verifying, by the verifying party, a path from the certificate authority trusted by the verifying party up to the public key certificate of the registration authority.

18. (Previously Presented) A method as recited in claim 17; wherein

the verifying party obtains the public key certificate of the registration authority from a public key certificate database of the issuing authority according to the registration authority name described on the public key certificate.

19. (Previously Presented) A method as recited in claim 17; wherein

the verifying party obtains the public key certificate of the registration authority described in an extended region of the public key certificate to be verified.

20. (Previously Presented) As method as recited in claim 11, further comprising the steps of:

sending, by the registration authority, a certificate invalidation request to the issuing authority of the public key certificate of the registration authority;

receiving, by the issuing authority, the certificate invalidation request; and

invalidating, by the issuing authority, the public key certificate of the registration authority.

21. (Previously Presented) A certificate authority to be used in a public key infrastructure including a plurality of end entities comprising:

(A) a registration authority for generating:

(A-1) a signature to contents to be registered with a public key certificate of each of the plurality of end entities; and

(A-2) a certificate issuing request including both the contents signed by the registration authority and a signature to the contents signed by the registration authority; and

(B) an issuing authority (12) connected to the registration authority through a network for generating, in response to the certificate issuing request, a public key certificate including:

(B-1) the contents signed by the registration authority;

(B-2) the signature to the contents signed by the registration authority;

(B-3) issuing contents to be issued by the issuing authority; and

(B-4) an issuing authority signature to the contents signed by the registration authority, the signature to the contents signed by the registration authority and the issuing contents issued by the issuing authority, the public key certificate being sent to the registration authority and registered within the registration authority.

22. (New) The method according to claim 11, wherein the public key certificate having been generated includes its own valid term, and wherein the registration authority is arranged to delete information on the public key certificate if the valid term has been ended.

23. (New) The method according to claim 11, wherein the registration authority is arranged to delete information on the public key certificate in response to a public key certificate invalidation request sent from the issuing authority.

24. (New) A method for generating a public key certificate of an end entity by a registration authority and an issuing authority in a public key infrastructure, comprising the steps of:

generating, by the registration authority, a signature to contents to be registered with a public key certificate having its own valid term, and a certificate issuing request including both the contents signed by the registration authority and a signature to the contents signed by the registration authority;

sending the certificate issuing request from the registration authority to the issuing authority;

generating, in response to the certificate issuing request by the issuing authority, a public key certificate including the contents signed by the registration authority, the signature to the contents signed by the registration authority, issuing contents to be issued by the issuing authority, and an issuing authority signature to the contents signed by the registration authority, the signature to the contents signed by the registration authority and the issuing contents issued by the issuing authority;

sending the public key certificate from the issuing authority to the registration authority for being registered within the registration authority;

deleting information, at the registration authority, on the public key certificate having been generated if the valid term has been ended; and

deleting information, at the registration authority, on the public key certificate having been generated in response to a public key certificate invalidation request sent from the issuing authority.